ELEN E6883: Introduction to Blockchain Technology

Homework 2

Tong Wu, tw2906

Problem 1

Section 1

False

Section 2

True

Section 3

True

Section 4

True

Section 5

True

Problem 2

Section 1

According to the hint, a_z satisfies the recurrence relation $a_z = pa_{z+1} + qa_{a-1}$, reform the equation in terms of $a_z - a_{z-1}$:

$$a_z - a_{z-1} = (\frac{q}{p})^{z-1}(a_1 - a_0) + a_0$$
$$a_z = \sum_{i=0}^{z-1}(\frac{q}{p})^{z-1}(a_1 - a_0) + a_0$$

Where the a_0 should be 1 in this case since the attacker has the same block as the chain (p=q):

$$\begin{aligned}
a_z &= \sum_{i=0}^{z-1}(\frac{q}{p})^{z-1}(a_1 - a_0) \\
&= \sum_{i=0}^{z-1}(\frac{q}{p})^{z-1}(a_1 - 1) + 1 \\
&= (a_1 - 1)\frac{1-(\frac{q}{p})^z}{1-\frac{q}{p}} + 1 \\
&= a_1 z - k + 1
\end{aligned}$$

$$\text{Assume } z \to \infty,\ a_z = 0:$$
$$\lim_{z\to\infty}(a_1 - 1)\frac{1-(\frac{q}{p})^z}{1-\frac{q}{p}} + 1 = 0$$

$$a_1 = 1 - \frac{1-\frac{q}{p}}{1-(\frac{q}{p})^z}$$
$$a_z = \begin{cases} (\frac{q}{p})^z, & \text{p} > \text{q} \\ \\ 1, & \text{otherwise} \end{cases}$$

Section 2

Since that the equation of the probability of an event with m time successes and n times of failures can be written as:

$$P = q^m p^n$$

In the trail, the last trail must be failure so the last successes is coming before the last failure, so there should be total $m + n + 1$ trails. Hence, it can be written as:

$$P(m) = \binom{m+n+1}{m} q^m p^n$$

Problem 3

Section 1

If a transaction from address X is included from the miner, then the pool will fork since the pool has the most of the hash power, which will create a longer chain in order to invalidates the chains contains the transaction from the address X. Hence, the miner will be informed that this block will be invalidated.

Section 2

The probability that the attacker successfully build the block is q^2. Hence, in order to avoid attacking, the payment amount should be:

$$(1-q^2)(\text{transaction fee} + \text{reward})$$

Where the total amount should be greater than the block reward, hence:

$$\begin{aligned}(1-q^2)(\text{transaction fee} + \text{reward}) &\geq \text{reward} \\ \text{transaction fee} &\geq \frac{\text{reward}}{1-0.2^2} \\ \text{transaction fee} &\geq \frac{12.5}{0.96} - 12.5 \\ \text{transaction fee} &\geq 0.5208\ \text{BTC}\end{aligned}$$

Problem 4

Section 1

Begin	End	Probability	Event
0’	0	$(1-\gamma)(1-\alpha)$	Honest miner mines a block on the main branch
0’	0	$\gamma(1-\alpha)$	Honest miner mines a block on the selfish miner’s block
0’	0	α	Selfish miner mines a block on the private branch
0	0	$1-\alpha$	Honest miner mines a block
1	0’	$1-\alpha$	Honest miner mines a block on the main branch, selfish miner publishes the private branch containing one block
2	0	$1-\alpha$	Honest miner mines a block on the main branch, selfish miner publishes the private branch containing two blocks
n	n+1	α	Selfish miner mines a block on the private branch
n	n-1	$1-\alpha$	Honest miner mines a block on the main branch

Section 2

Begin	End	Probability	Reward
0’	0	$(1-\gamma)(1-\alpha)$	2
0’	0	$\gamma(1-\alpha)$	1
0	0	$1-\alpha$	1